REMARKS

Claims 1-21 are presented for further examination. Claims 1, 10, 13, 16, 19, and 21 have been amended.

In the Office Action mailed June 26, 2008, the Examiner rejected claims 1-21 under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 5,852,290 ("Chaney") in view of U.S. Patent No. 6,311,204 ("Mills").

Applicants respectfully disagree with the basis for the rejection and request reconsideration and further examination of the claims.

Claim Rejection

An aspect of the described and claimed embodiments is the enhanced security provided by having both a common key store and secret key store formed on the same integrated circuit. Common keys are received in an encrypted form and must be decrypted before they can be used. In prior designs, remote smart cards are read by the decoder to decrypt encrypted control words. In the smart card approach, decrypted control words are thus available for detection by hackers across an open interface between the smart card and the decoder as discussed in the present specification. The claimed embodiments of the present disclosure overcome the potential security breach that can happen when the decrypted control words are recorded and provided to other users by another communication channel such as the internet in which any recipient is thereby enabled to descramble the broadcast signal.

In Chaney, U.S. Patent No. 5,852,290, a smart card 180 is used to interface with a card reader 190 to enable a user to access a pay-TV service (see column 4, lines 5-9). Chaney thus suffers from the potential security breach by having an open interface with a card reader.

Similarly, Mills, U.S. Patent No. 6,311,204, utilizes a smart card that interacts with a smart card interface 80 to decode or decrypt service keys that are used to de-encrypt control words for descrambling a TV signal. The interface 80 of Mills can enable a hacker to obtain the decrypted signal as described above.

Claim 1 recites a semiconductor integrated circuit that includes an input interface, a processing unit to receive encrypted broadcast signals and control signals, a first decryption

circuit communicating with a common key store in the integrated circuit and a second decryption circuit communicating with a secret key store in the integrated circuit. Thus, as claim 1 recites, the circuit is arranged such that the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key, and to provide the common key to the common key store over an internal bus. Claim 1 further recites that the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

The current invention, as claimed in claim 1, describes a monolithic integrated circuit in which control signals, broadcast signals and common keys are all broadcast in encrypted form. The common keys are encrypted according to a secret key, which may be specific to a given device. The control signals are decrypted by the common keys. The broadcast signals are decrypted in accordance with the control signals.

A key aspect of the invention is that the circuit is monolithic, with all components connected by internal buses to avoid any insecure interfaces, coupled with the fact that the only route to placing common keys in the common key store is to input the common keys in encrypted form for decryption in accordance with a secret key and provide them to the common key store over an internal bus. This enforces, in hardware, the need to know the secret key and the common key in order to operate the device.

The Examiner objects to all the claims in view of a combination of the documents Chaney and Mills. I believe there is an argument against combining Chaney and Mills.

Chaney describes a system in which a smartcard contains an onboard descrambler, which receives a key from an onboard processor. The Examiner refers to column 5, lines 50-67 and column 6, lines 55-67 as disclosing a decryption circuit arranged to receive encrypted control signals from the input interface and decrypting the control signals in accordance with a common key from a common key store. However, these portions of Chaney refer to ECM data (i.e. control signals) and how this is used to decrypt broadcast data (i.e. video/audio). The term "common key" as used in the claims is specific to a key that is used to descramble control signals. The decryption of control signals (such as ECMs) is not disclosed by the portion of Chaney referred to by the Examiner.

If one interprets Chaney in view of column 11, lines 15-20 it seems that this document does disclose ECM data (i.e. control signals) being broadcast in encrypted form and that a key (a common key as we mean it), provided on the smartcard, is needed to decrypt the ECM data. Therefore, Chaney discloses a common key being provided on the smartcard but does not disclose a system for receiving common keys provided by broadcast.

Neither does Chaney disclose the only route to placing the common key in the common key store being to input the common key in encrypted form for decryption in accordance with a secret key and provide it to the common key store over an internal bus. There is no reason why it would do so since the whole point of a smartcard system is that the common key, used to decrypt the ECM control signals, is stored on the smartcard. When it is desired to change the common key, typically the smartcards are reissued to customers with new keys pre-stored on them. The hardware route used to store the common key is irrelevant in a smartcard system in which the main security offered is their replaceability.

The Examiner then turns to Mills to cure the defects of Chaney. Mills describes a system in which a secret on-card key is used to decrypt a "service key" which is then used to decrypt subsequent ECMs (i.e. a secret key that is used to decrypt a common key). The Examiner asserts that this document also discloses a system in which the only route to placing the common key in the common key store is to input the common key in encrypted form for decryption in accordance with a secret key and to provide it to the common key store over an internal bus. However, this does not appear to be the case.

Column 11, lines 30 to 50 of Mills describe how encrypted service keys are contained within EMMs and used to decrypt ECMs. However, Mills is silent on where the service keys are stored on the smartcard (if at all) and the route in which they are passed to the smartcard. Mills simply says that a DMA technique may be used to implement the transfer of EMM and ECM data from the system to the smartcard.

Firstly, it is noted that DMA techniques do not in any way guarantee that the encrypted common key must be decrypted before being stored. In fact, DMA allows only for block transfers of data and therefore if the DMA transfer results in storage of the EMM data and the service keys, they will be stored in encrypted form. This is contrary to the inventive concept

because the whole point is that the common keys are stored before use and in order to store them, they must first be decrypted according to the secret key. This ensures, by hardware arrangement, that the integrated circuit cannot be used without knowledge of both the secret key and the common key. Therefore, Mills does not provide the feature of the only route to placing the common key in the common key store being to input the common key in encrypted form for decryption in accordance with a secret key and to provide it to the common key store over an internal bus. At best it implies that the service key may be stored in encrypted form.

Secondly, transfer of the EMM to the smartcard takes place under the control of the processor (even DMA access requires the processor to initiate the transfer). This means that the path of the EMM, which contains the service keys, is dictated by software and not hardware. This is far less secure than the current invention which is hardwired by the internal bus to ensure only one route for the common key to be provided to the common key store. Software arrangements and processors can be spoofed to alter the data being stored, or the location to which that data is passed. This would allow a hacker to identify the secrets being passed between the main system and the smartcard of Mills.

More particularly, the current claimed embodiments relate to a conditional access system that does not rely on smartcards. In smartcard systems, such as the one discussed in the opening pages of the present application (and the systems of both Mills and Chaney) control words are broadcast in encrypted form. The control words instruct a descrambler as to how to descramble the encrypted audio/video data. Common keys (i.e. the keys required to decrypt the control words) are then distributed to each user, typically by sending them a physical smartcard, containing the common keys. In any case, the smartcard contains secrets to allow decryption of the broadcast data.

A totally different approach is used in the current claimed embodiments. A smartcardless system is achieved by providing all the features of claim 1; in particular, an integrated circuit with a secret key store for storing a secret key being unique to a particular integrated circuit. The common keys are then broadcast encrypted using secret keys unique to each circuit or to a group of circuits, and so are broadcast in millions of different encrypted forms (ideally one form to each recipient or group of recipients). An advantage of having a

system that does not require a smartcard is the removal of any vulnerable interfaces over which sensitive data can be uncovered by a hacker.

There is no teaching in the prior art of overcoming this by providing an integrated monolithic circuit with the features of claim 1. Indeed both Chaney and Mills suffer from the very deficiencies the present invention seeks to solve, namely sensitive information is passed over an insecure interface between the smartcard and the main system. In order for the skilled person to be motivated to remove all the vulnerable interfaces and produce the current invention he would need to appreciate that a smartcardless approach is desirable and viable. This is simply not taught by the cited art which both use smartcards. Indeed, it should also be noted that Chaney discloses alternative methods for dealing with possible exposure of sensitive information at the smartcard interface (see column 8, line 53). This teaches towards using complex timing arrangements and passing additional data over the interface, and away from the removal of the vulnerable interface altogether, as achieved by the current invention.

Thus, there is no teaching or suggestion in either Mills or Chaney, taken alone or in any combination thereof, of having both the common key store and the secret key store formed in the same integrated circuit. Applicants respectfully submit that claim 1 is allowable. Claims 2-9, each of which depend from or rely upon the recitation of claim 1, are allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

Independent claims 10, 13, 16, and 19 each recite the common key store and the secret key store formed in the monolithic device or semiconductor integrated circuit. Applicants respectfully submit that each of these independent claims is allowable for the reasons discussed above with respect to claim 1. All claims depending from these independent claims are respectively allowable for the features recited therein as well as for the reasons why their independent claims are allowable.

In view of the foregoing, applicants respectfully submit that all of the claims in this application are now in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, the Examiner is urged to contact the undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve

prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

Respectfully submitted,

SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:jl

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1195460_2.DOC